An examination of the fraud liability shift in consumer card-based payment systems

Duncan B. Douglass

Introduction and summary

In the absence of a significant (and right now unforeseeable) shift in the retail payments landscape in the United States, consumers will continue to reach consistently (and often) for their debit and credit cards. They will use these cards when paying for goods and services in face-to-face, Internet, mail order, and telephone order transactions. Likewise, criminals will continue to use tried-and-true tactics and will develop innovative methods to perpetrate payment card fraud.

At the intersection of consumers conducting legitimate card transactions and fraudsters pursuing their illegal ends is a tangled web of public laws and private card network rules. These laws and rules allocate fraud risk among the consumers, card issuers, and merchants participating in card-based payment systems. In theory, one would hope that these laws and rules for payment card transactions are thoughtfully designed to encourage behavior that minimizes fraud losses to the system as a whole. In reality, systemwide fraud reduction is often not the principal objective behind particular public laws or private rules affecting fraud liability allocation. Consequently, these laws and rules may fail to promote efficient fraud avoidance; indeed, in some instances, they may actually *discourage* fraud avoidance.

Defining the issue

The first step in evaluating the efficiency of fraud liability allocation rules in current card-based payment systems is to define the issue. Doing so requires an understanding of the difference between identity theft and common payment card fraud, as well as an understanding of the workings of the card-based payment systems at issue.

Identity theft versus fraud

News stories abound about identity theft resulting from dumpster divers absconding with old bank statements and criminals rifling through mail and intercepting credit card offers. Further, email accounts are barraged with phishing attempts and other web-based schemes craftily designed to lure consumers into revealing personal identification information that can be used for nefarious purposes. Typically, the fraudsters intend to use the ill-gotten fruits of their snooping to impersonate their victims and access their credit or asset accounts. This is identity theft, and it is an increasingly pervasive problem in the United States and throughout the world. During 2007, Consumer Sentinel, a network that collects information about consumer fraud and identity theft from the Federal Trade Commission and over 125 other organizations, recorded 258,427 identity theft complaints.[1]

Identity theft is distinguishable from common financial fraud. Identity theft is generally defined as "the use of personal identifying information to commit some form of fraud."[2] In contrast, fraud is simply "[a] knowing misrepresentation of the truth ... to induce another to act to his or her detriment."[3] As noted in the definition of identity theft, fraud is typically the end goal of identity theft. However, often fraud is committed without antecedent theft of Social Security numbers or other assumption of identity. Along with the cases of identity theft reported in 2007, 555,472 cases of non-identity-theft-related fraud were reported during the same year.[4] Given that card-based payment systems (and other payment systems, for that matter) seek to prevent monetary fraud perpetrated through the system regardless of how the information used to perpetrate the fraud was obtained, here I focus on the broader category of payments fraud—whether or not

Duncan B. Douglass is a partner at Alston and Bird LLP, practicing in the areas of corporate and retail payment systems.

it is precipitated by identity theft. There is no need to steal another person's identity to perpetrate simple payment card fraud—all the perpetrator needs to do is obtain a person's payment card or payment card information.[5]

Distinguishing fraud from identity theft is important to the discussion that follows for two reasons. First, fraud is broader and more pervasive than identity theft. Second, the means of preventing fraud in the initiation of payments, and the appropriate allocation of losses that result from payments fraud, are generally not dependent on whether the fraud resulted from identity theft or from a simpler card/data theft incident. There is no doubt that consumers who fall victim to identity theft experience significant nonmonetary losses in addition to the losses resulting from the fraudulent transactions. These include the opportunity costs of time spent disputing fraudulent claims, closing existing accounts, and opening new accounts.[6] However, public laws and private rules governing card payment systems are not capable of preventing such costs to consumers because these costs are wholly external to the payment system itself.

Payment systems fraud generally versus signature-based card fraud

Having distinguished identity theft from payments fraud and clarified that this discussion is concerned with the latter, it is worth making the distinction between payment systems fraud generally and payment systems fraud perpetrated through means of a signature-based access device. This distinction is important because public law treats access device fraud differently than other types of payment systems fraud. Moreover, private card network rules related to fraud are generally different for signature-based card products than for other payment products (including card products based on a PIN, or personal identification number). For the purposes of this article, I limit my consideration to signature-based consumer debit cards (which are directly or indirectly linked to, and draw funds for settlement from, a consumer asset account) and credit cards (which are linked to, and draw funds for settlement from, a line of credit extended by the card issuer). These types of debit and credit cards are issued for acceptance on the major credit card networks in the United States: Visa, MasterCard, American Express, and Discover.

Of course, there are other payment card forms and other types of accounts that can be accessed using payment cards. These include wireless technology key fobs, biometric account access that uses no card at all, and prepaid cards that access a different type of account altogether. Again, I only discuss signature-based debit and credit cards here because these devices and the accounts they access remain the most prevalent in the retail payment systems marketplace.

Allocation of payment card fraud liability: Public laws and private rules

Determining which party to a given fraudulent payment card transaction has liability for the fraud requires an understanding of both the applicable public legal framework and the private card network rules. A fundamental assumption in this article (and many others, although the point is often unstated) is that the actual wrongdoer—the perpetrator of the fraud—will be unavailable for recovery, and so one of the innocent parties involved in the transaction must be asked to bear the resulting loss. Absent any public laws or private rules to the contrary, the cardholder would be the risk bearer by default unless a benevolent merchant or card issuer agreed to absorb the loss. Luckily enough for cardholders, both public laws and private card network rules intervene to protect cardholders and to reallocate liability for fraud losses among other participants to a fraudulent card payment transaction.

Public law

The public law framework that serves to protect consumer users of credit and debit cards from bearing the full brunt of fraud losses associated with lost or stolen access devices are as follows: the Truth in Lending Act (TILA), together with Regulation Z, and the Electronic Fund Transfer Act (EFTA), together with Regulation E.[7] Historically, Congress has shown a fair degree of restraint in tinkering with TILA and the EFTA. Instead, Congress has allowed the Board of Governors of the Federal Reserve System to use its regulatory authority to extend appropriate consumer protections to new payment products and account structures through revisions to Regulation Z and Regulation E.[8]

Likewise, the Federal Reserve Board generally has taken a measured approach in amending Regulation Z and Regulation E to address market developments (for example, transactions initiated by mobile phone) and new funding sources accessed by payment cards (for example, prepaid accounts held by the card issuer in an omnibus account structure).[9] The Federal Reserve Board expressly acknowledged its restrained approach to expanding regulations when it promulgated the interim final rule extending Regulation E coverage to payroll cards, noting that the Board was not extending coverage more broadly to prepaid cards because "coverage of such products could impede the development of other card products generally."[10]

Truth in Lending Act and Regulation Z

Under TILA and Regulation Z, cardholder liability is capped at $50 for all unauthorized transactions, regardless of whether the fraud occurs in a single transaction or multiple transactions and regardless of when the cardholder learns of the loss or theft of the card or reports the loss or theft to the card issuer.[11] The cardholder has no liability for unauthorized activity after alerting the card issuer of the loss or theft of the card (that is, the cardholder's liability is limited to the lesser of $50 or the amount of fraud committed before the cardholder notifies the card issuer of fraud or the loss or theft of the credit card).[12] Regulation Z defines unauthorized use in connection with a credit card as use "by a person, other than the cardholder, who does not have actual, implied, or apparent authority for such use, and from which the cardholder receives no benefit."[13] Unauthorized use of a credit card includes both physical use of a lost or stolen card or fraudulent use of information from a credit card, whether or not the actual device has been lost or stolen.[14] Thus, fraudulent use of a credit card number and expiration date to conduct a card-not-present transaction over the Internet constitutes "unauthorized use" according to Regulation Z.

Electronic Fund Transfer Act and Regulation E

The EFTA and Regulation E place a floating cap on a consumer cardholder's liability for unauthorized debit card use under which the maximum liability amount is determined when the cardholder notifies the card issuer of the loss or theft of the card used to perpetrate the fraud. If the cardholder notifies the card issuer within two business days of learning of the loss or theft of the debit card, the cardholder's maximum liability is limited to the lesser of the actual amount of unauthorized transfers or $50.[15] If the cardholder fails to notify the card issuer within two business days of learning of the loss or theft, the cardholder's maximum liability is $500, of which only $50 can be attributable to fraud occurring during the first two business days after the cardholder learned of the loss or theft.[16] In addition, if the cardholder fails to notify the card issuer of unauthorized activity within 60 days after the card issuer sends a periodic statement reflecting the unauthorized transactions, subject to the $50 and $500 liability caps, the cardholder has unlimited liability for fraudulent transactions occurring after the 60th day.[17]

It is worth noting that negligence of the cardholder in safeguarding the debit card is not a basis for the card issuer to impose greater liability on the cardholder than is otherwise permissible under the EFTA/Regulation E.[18] Regulation E defines an unauthorized electronic funds transfer as a transfer "initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefit."[19] Unauthorized use under Regulation E includes fraudulent use of information from a debit card, including card number and expiration date, to initiate an electronic funds transfer.

Card network fraud liability rules

TILA/Regulation Z and the EFTA/Regulation E set a baseline maximum of consumer cardholder liability for fraudulent transactions conducted using a credit card or debit card.[20] The effect of this public law regime is to require the card issuer to absorb all fraud liability in excess of the maximum cardholder liability allowed under law. Given the stated purposes of TILA/Regulation Z and the EFTA/Regulation E—to protect consumers—it is not surprising that these laws are not concerned with further allocation of fraud liability after shifting responsibility from the cardholder to the card issuer.[21] The card network rules both enhance the baseline cardholder protections established by TILA/Regulation Z and by the EFTA/Regulation E and further allocate fraud liability from card issuers to merchants based on a complicated set of rules that vary based on the type of transaction at issue. The card networks enhance the cardholder protections offered under TILA/Regulation Z and the EFTA/Regulation E through their "zero liability policies."[22] The card networks allocate fraud liability risk between card issuers and merchants based upon detailed dispute resolution rules, which take into account at least some element of the respective parties' compliance with network rules designed to detect and deter attempted fraudulent transactions.

Whether the card issuer or the merchant to a particular fraudulent transaction ultimately will be liable for the fraud losses depends on if the merchant followed the payment card rules in connection with the particular transaction. There are numerous permutations of rule requirements for all manner of transaction types. One of the most significant determinants of whether the card issuer or the merchant in a particular transaction will be responsible for fraud is whether the transaction is a face-to-face transaction (a "card-present transaction") or a transaction conducted over the Internet, by mail, or by telephone (a "card-not-present transaction").

If one distills the standard requirements across the card networks to their essence, it is generally true that a merchant engaging in a card-not-present transaction may only successfully overcome a cardholder/card issuer allegation that the transaction was the result of fraud if the merchant 1) performed an address

verification at the time the transaction was authorized (that is, verified that the person conducting the transaction could validate the billing address associated with the payment card being used); 2) delivered the purchased merchandise to an address that matches the address validated through the address verification; and 3) obtained proof that the purchased goods were delivered to the verified address. If the merchant cannot satisfy these requirements, the card network rules typically shift fraud liability from the card issuer to the merchant. Contrast this to the card-present transaction environment, where a merchant may successfully defend a transaction disputed by the cardholder or card issuer as fraudulent by demonstrating that the card was present at the point of sale and by producing a signed transaction receipt. In the event of such a successful defense, the card issuer typically will be held accountable for the fraud losses.

Do current fraud liability allocation rules create incentives that minimize systemwide fraud losses?

A shorthand way to look at default liability allocation under public law and private rules of the payment card schemes is as follows: 1) Consumers rarely bear meaningful liability for fraudulent transactions unless they benefited from the fraud; 2) issuers typically bear liability for fraud losses perpetrated in card-present transactions; and 3) merchants generally bear liability for fraud losses perpetrated in card-not-present transactions. Taking a systemwide approach to fraud in card-based payment systems, the natural question that follows from the current status quo is whether the rules for fraud liability allocation result in efficient outcomes: That is, are the parties to each payment card transaction vested with appropriate incentives in the form of fraud liability risk to encourage each to take reasonable steps to minimize fraud losses viewed from the perspective of the payment system as a whole?

Cardholder liability for fraudulent transactions

There is little doubt that cardholders' carelessness in protecting their own card information contributes to the incidence of payment card fraud. A recent study commissioned by Canada's Interac Association found that 60 percent of Canadians do not shield their PIN entry at automated teller machines (ATMs) or point-of-sale terminals when they believe no one is watching them and that 37 percent do not shield their PIN entry even when they believe someone can see them entering it.[23] The extent to which cardholders are regularly negligent in protecting their own card information from potential fraudsters is debatable. On the one hand, cardholders surely do not wish to invite fraud. On the other hand, while cardholders may not be aware of the nuanced differences in fraud liability protections available under public laws and private rules,[24] it would be difficult for cardholders not to be aware of their protections under the zero liability policies prominently and repeatedly promoted by the card networks.[25]

Assuming most consumers understand, at least in some abstract sense, that they are protected from liability for fraud losses regardless of their level of diligence in safeguarding their own information, one wonders whether a greater deductible on the first-dollar insurance coverage mandated by the card networks through zero liability policies would reduce the incidence of fraud by encouraging appropriate risk-avoiding behavior.[26] As it currently stands, the major card networks' zero liability policies (and even the very low deductibles payable by cardholders under public law) leave in place a significant risk of moral hazard[27] that almost certainly, at least at the margins, contributes to overall systemwide fraud losses.

Notwithstanding what appears to be somewhat low-hanging fruit in the effort to achieve systemwide fraud reduction, there are two significant challenges—both likely insurmountable—that make increasing cardholder liability highly unlikely regardless of the efficiency in the outcome it may engender. The first challenge is the increasing trend among legislators and regulators to enact payment-system-related public laws that offer greater consumer protection regardless of the efficiency of the fraud-related outcomes these laws may create.[28] A reversal of this trend among legislators, in particular, is unlikely given increased public attention on consumer protections in payment systems.

The second challenge is the need, critical to broad-based user adoption and acceptance of any payment system, for the users to have confidence in the system's security and safety. Card network operators are constantly searching for ways to induce greater cardholder confidence in the security of making card-based payments—which they hope will result in a correlative increase in transaction volume across the payment system.[29] Designing a card-based payment system that increases consumer liability for fraudulent transactions would likely undermine confidence in the system overall and result in reduced transaction volume—the opposite of the desired effect. Given these counterincentives among those who promulgate the applicable public laws and private rules, increased cardholder liability is likely not a viable option for improving the overall efficiency of fraud liability allocation rules.

Liability for fraudulent transactions: Card issuer versus merchant

If increasing cardholder liability is an improbable outcome of any fraud-reducing reforms to card payment systems at the level of either public law or private rules, then we are left to consider whether adjustments to the allocation of fraud liability between card issuers and merchants under current card network rules might have a desirable effect in reducing systemwide fraud losses. As described previously, the card issuers generally bear fraud liability in card-present transactions and merchants generally bear fraud liability in card-not-present transactions.

In the card-present context, existing card network rules may provide inadequate incentives for merchants to take efforts to detect and deter fraudulent transactions. Generally, so long as the presented card is swiped through the point-of-sale terminal and a signature is obtained on the transaction receipt, the merchant will not bear the loss if the transaction is subsequently challenged as fraudulent. Consequently, the marginal economic benefit to merchants of deploying additional fraud prevention measures, even if effective measures are made available by card issuers and card networks, may well not justify the costs to the merchant of implementation because the merchant stands to gain little. Fraud detection measures in traditional brick-and-mortar sales channels today include the examination of the card for evidence of tampering and a comparison of the signature on the transaction receipt to the signature on the back of the card (although many merchants' employees do not even glance at the card presented for payment).

In contrast, in the card-not-present environment, existing card network rules may create disincentives for card issuers to support and induce their cardholders to participate in fraud prevention efforts. Nowhere is this more evident than in the surprisingly low adoption of card networks' payer authentication programs.[30] Visa and MasterCard have each developed and actively promoted services designed to assist Internet merchants in authenticating payers—for Visa the Verified by Visa program and for MasterCard the MasterCard SecureCode program. Under both programs, a preenrolled cardholder conducting a card-not-present transaction at a participating merchant is asked to provide an authenticating password in a secure pop-up window or frame linked to the card issuer.[31] The pop-up window or frame in which the cardholder is asked to provide the password displays a phrase or image preselected by the cardholder so that the cardholder can validate that the pop-up or frame is linked to the card issuer.[32] This bidirectional layer of additional authentication not only deters fraud, but card network rules provide that it also shifts fraud liability risk from the merchant to the card issuer for the verified transaction.

One might think merchants would eagerly adopt these additional security measures and embrace the attendant liability shift to the card issuer for Internet transactions. However, online merchants that have attempted to require customers to enroll in such programs have invoked the ire of their customers. Card issuers have little incentive to expend resources or risk cardholder backlash by requiring participation in such programs given that the benefit would accrue primarily to the merchant, with the added offense of shifting transaction fraud liability to the issuer.[33] In other words, card network rules appear to create the same dilemma of moral hazard in allocating fraud losses between card issuers and merchants in both card-not-present and card-present transactions as is created by public laws and private rules that insulate cardholders from fraud liability.

Conclusion

Empirical evaluation suggests that current public law regimes and private card network rules may fail to create appropriate incentives for cardholders, merchants (in card-present transactions), and card issuers (in card-not-present transactions) to adopt fraud-reducing practices. These rules may also discourage fraud-avoiding behavior in certain circumstances because of the associated costs and efforts involved and the limited benefit to be gained by the party undertaking those costs and efforts. This is not to say the current architecture of public laws and private rules is fundamentally flawed or in need of reworking from the ground up. As Robert Ballen and Thomas Fox have argued, the current system in which public law and private rulemaking collaborate to create fraud liability rules is capable of functioning effectively to achieve efficiency in payment systems.[34] However, it may be time to reevaluate the incentives created by current card network rules in allocating fraud liability among transaction participants to better align risks with the parties that are able to make efficient decisions regarding how to mitigate them. Increasing cardholder liability is likely not on the table for consideration, but efficiency gains in terms of reduced systemwide fraud losses may well be possible through relatively minor adjustments to the allocation of liability between merchants and card issuers.

NOTES

[1]See Federal Trade Commission, 2008, *Consumer Fraud and Identity Theft Complaint Data: January–December 2007*, report, Washington, DC, February, available at www.ftc.gov/opa/2008/02/fraud.pdf.

[2]Federal Deposit Insurance Corporation, 2004, "Putting an end to account-hijacking identity theft," report, Washington, DC, December 16, available at www.fdic.gov/consumers/consumer/idtheftstudy/background.html.

[3]See Bryan A. Garner (ed.), 1999, "Fraud," *Black's Law Dictionary*, 7th ed., Eagan, MN: West Publishing Company, p. 670.

[4]See Federal Trade Commission (2008).

[5]Card payment fraud can be perpetrated in person, if the fraudster has obtained the actual payment card, or over the Internet or via mail or telephone order, if the fraudster possesses the victim's name, card account number, expiration date, and card identification number (CID)—also called card verification value (CVV2) or card verification code (CVC2), depending on the card scheme at issue. Many online retailers will accept, and card issuers will approve, transactions in which significantly less information is provided through the online payment channel.

[6]One author has suggested that the victims of identity theft spend an average of 40 hours resolving fraudulent transactions and other issues relating to the identity theft. See Erin Fonté, 2007, "Who should pay the price for identity theft?," *Federal Lawyer*, September, pp. 24–25.

[7]The Truth in Lending Act, which is contained in Title I of the Consumer Credit Protection Act, as amended (15 U.S.C. § 1601 et seq.), was enacted by Congress in 1968 as a consumer protection measure requiring clear disclosure of key terms and costs of lending arrangements. The Federal Reserve Board has promulgated Regulation Z to implement TILA pursuant to authority granted under 15 U.S.C. § 1607. The Electronic Fund Transfer Act (15 U.S.C. § 1693 et seq.) was enacted by Congress in 1978 to establish rights, liabilities, and responsibilities of consumers who use and financial institutions that offer electronic fund transfer services. The Federal Reserve Board has promulgated Regulation E to implement the EFTA pursuant to authority granted under 15 U.S.C. § 1693b.

[8]This historical trend has been threatened as of late. During 2007 and 2008, Congress became much more active in proposing and promoting consumer protection bills. See, for example, Credit Cardholders' Bill of Rights Act of 2008 (H. R. 5244) and Credit Card Reform Act of 2008 (S. 2753).

[9]Like Congress, the Federal Reserve Board was much more active in addressing payment market developments during 2008 than it had been historically. For example, on May 19, 2008, the Federal Reserve Board proposed an uncharacteristically sweeping set of amendments to Regulation Z. See Board of Governors of the Federal Reserve System, 2008, "12 C.F.R. Part 226, [Regulation Z; Docket No. R–1286], Truth in Lending; proposed rule," *Federal Register*, Vol. 73, No. 97, May 19, pp. 28866–28901. Much of this activity likely stems from the *push* the Federal Reserve Board is feeling from Congress. The rapid-fire succession of consumer protections bills from Congress appears to have served as a sort of notice to the Federal Reserve Board to regulate or get out of the way.

[10]Board of Governors of the Federal Reserve System, 2005, "Electronic fund transfers: Interim final rule; request for public comment," notice, Docket No. R-1247, Washington, DC, December 30, available at www.federalreserve.gov/boarddocs/press/bcreg/2005/20051230/attachment2.pdf.

[11]See 12 C.F.R. § 226.12(b)(1).

[12]See *id*.

[13]2 C.F.R. § 226.12 n.22.

[14]See Mark Furletti and Stephen Smith, 2005, "The laws, regulations, and industry practices that protect consumers who use electronic payment systems: Credit and debit cards," Series on Fraud, Error, and Dispute Protections, Federal Reserve Bank of Philadelphia, Payment Cards Center, discussion paper, No. 05-01, January, available at www.philadelphiafed.org/pcc/papers/2005/ConsumerProtectionPaper_CreditandDebitCard.pdf.

[15]See 12 C.F.R. § 205.6(b)(1).

[16]See 12 C.F.R. § 205.6(b)(2).

[17]See 12 C.F.R. § 205.6(b)(3).

[18]12 C.F.R. pt. 205, Supp. I, § 205.2, cmt. 2(a), note 2.

[19]12 C.F.R. § 205.2(m).

[20]As mentioned in the subsection titled payment systems fraud generally versus signature-based card fraud, the present discussion is limited to signature-based debit and credit cards and card networks—meaning that the card network rules considered are those of Visa U.S.A. Inc., MasterCard International Inc., American Express Travel Related Services Company Inc., and Discover Financial Services.

Readers may note that TILA/Regulation Z apply the $50 liability cap to all cardholders, not just consumers, while the EFTA/Regulation E apply the limitations on liability only to consumer cardholders. While this is a meaningful distinction, we will assume for purposes of the present discussion that the victimized cardholder is a consumer, whether the card at issue is a credit card or a debit card.

[21]According to 15 U.S.C. 1601, "it is the purpose of [TILA] ... to protect the consumer against inaccurate and unfair credit billing and credit card practices." According to 15 U.S.C. 1693, "the primary objective of [the EFTA] ... is the provision of individual consumer rights."

[22]Regulation Z expressly provides that an agreement between a cardholder and the card issuer may impose lesser liability on the cardholder than is provided for under Regulation Z. See 12 C.F.R. § 226.12(b)(4). Similarly, Regulation E acknowledges that a cardholder and card issuer may agree to a lower cardholder's liability limit than the Regulation E default. See 12 C.F.R. § 205.6(b)(6). Each of Visa, MasterCard, American Express, and Discover has enacted some form of zero liability policy. The ultimate effect is that, except in very limited circumstances, a card issuer is required to assume, on behalf of its cardholders, even the amount of fraud liability permitted to be passed on to the cardholder under applicable public laws.

[23]See Glenbrook Partners LLC, 2006, "Survey shows Canadians not shielding their debit card PIN regularly," *Payments News*, October 19, available at www.paymentsnews.com/2006/10/survey_shows_ca.html.

[24]Commentators have noted that consumers are unaware of the different regulatory protections that apply based on the source of funding supporting a payment card transaction. See, for example, Marianne Crowe, Scott Schuh, and Joanna Stavins, 2006, "Consumer behavior and payment choice: A conference summary," Public Policy Discussion Papers, Federal Reserve Bank of Boston, discussion paper, No. 06-1, available at www.bos.frb.org/economic/ppdp/2006/ppdp061.pdf, and Furletti and Smith (2005).

[25]For example, Visa's website informs users of its credit cards and signature-based debit cards that "Visa will always protect you from unauthorized use." See http://usa.visa.com/personal/security/visa_security_program/zero_liability.html#anchor_2. Likewise, MasterCard advises cardholders that "your card issuer won't hold you liable in the event of an unauthorized use of your U.S.-issued MasterCard card." See www.mastercard.com/us/personal/en/cardholderservices/zeroliability.html.

[26]The same argument applies, albeit to a slightly lesser degree, to the very low deductibles payable by cardholders in connection with fraud loss insurance mandated by TILA/Regulation Z and the EFTA/Regulation E. In order to truly cause cardholders to take note of their liability exposure and adjust their behavior appropriately, the cardholder deductible would likely need to rise to a level exceeding the current public law maximums.

[27]Moral hazard has been defined as "the tendency for the insurance plans to encourage behavior that increases the risk of insured loss" by Allard E. Dembe and Leslie I. Boden, 2000, "Moral hazard: A question of morality?," *New Solutions,* Vol. 10, No. 3, pp. 257–279. That definition is consistent with the use of the term for this discussion. If a participant in a given payment system has no risk of loss due to fraudulent transactions, that participant may have little incentive to take actions, even of the simplest nature, to avoid or reduce the likelihood of fraud occurring.

[28]Without broadening the discussion to politics in general, recent proposals in Congress to enhance consumer protection laws that would increase substantially the costs to lenders of extending credit—as well as recent amendments to Regulation Z proposed by the Federal Reserve Board to do the same—support this proposition. See note 8.

[29]See, for example, Jenny C. McCune, 2000, "Shop the web without the worry—Companies reduce cardholders' liability," *Bankrate.com*, June 19, available at www.bankrate.com/brm/news/cc/20000619.asp.

[30]See CyberSource Corporation, 2008, *9th Annual Online Fraud Report*, 2008 ed., Mountain View, CA. This report comments on the relative slow adoption of payer authentication programs since 2003, notwithstanding significant expressions of interest by Internet merchants since 2003.

[31]See Federal Reserve Bank of Philadelphia, Payment Cards Center, 2003, "After the hype: E-commerce payments grow up," discussion paper, No. 03-12, available at www.philadelphiafed.org/pcc/conferences/2003/eCommerce_062003.pdf (see, in particular, the summary of the presentation by Steven W. Klebe, titled "Online fraud: The stakes are rising").

[32]See *id*.

[33]See, for example, Josh Leyden, 2008, "Net shoppers bullied into being verified by Visa," *The Register*, August 7, available at www.theregister.co.uk/2008/08/07/verified_by_visa_compulsion/.

[34]Robert G. Ballen and Thomas A. Fox, 2008, "The role of private sector payment rules and a proposed approach for evaluating future changes to payments law," *Chicago Kent Law Review*, Vol. 83, No. 2, pp. 937–952.